Keamanan Jaringan Komputer

Tugas Reconnaissance

Jan William Tarigan

09011281520114

1) Pemerintahan

- https://www.kemenkumham.go.id

Web Server : Apache

Operating Systems : Apache/2.4.7 (Ubuntu)

Framework : - Adobe Enterprise Cloud

- GlobalSign Domain Verification

- PHP

- Perl

Network

Site	https://www.kemenkumham.go.id	**Netblock Owner**	PT Indonesia Comnet Plus
Domain	kemenkumham.go.id	**Nameserver**	ns2.kemenkumham.go.id
IP address	103.111.28.80 (VirusTotal)	**DNS admin**	telematika@kemenkumham.go.id
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	*unknown*	**Nameserver organisation**	*unknown*
Organisation	*unknown*	**Hosting company**	PT. Indonesia Comnets Plus
Top Level Domain	Indonesia (.go.id)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

2) Luar Negeri

- https://www.kemenkumham.go.id

Web Server : Citrix NetScaler

Operating Systems : -

Framework : - ASP.NET 4.0

-Classic ASP

-ASP.NET MVC

-ASP.NET Ajax

-Shockwave Flash Embed

Site	https://www.bet365.com	**Netblock Owner**	Hillside New Media Net
Domain	bet365.com	**Nameserver**	a1.uberns.com
IP address	5.226.176.16 (VirusTotal)	**DNS admin**	td@bet365.com
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	markmonitor.com	**Nameserver organisation**	whois.wildwestdomains.com
Organisation	bet365 Group Limited, United Kingdom	**Hosting company**	*unknown*
Top Level Domain	Commercial entities (.com)	**DNS Security Extensions**	*unknown*
Hosting country	UK		

3) Dalam Negeri

- https://www.bola.net

Web Server : nginx

Operating Systems : FreeBSD

Framework : - PHP

Network

Site	https://www.bola.net	**Netblock Owner**	PT. KAPANLAGI.COM NETWORKS
Domain	bola.net	**Nameserver**	ns-229.awsdns-28.com
IP address	203.12.21.11 (VirusTotal)	**DNS admin**	awsdns-hostmaster@amazon.com
IPv6 address	*Not Present*	**Reverse DNS**	*unknown*
Domain registrar	godaddy.com	**Nameserver organisation**	whois.markmonitor.com
Organisation	ID	**Hosting company**	*unknown*
Top Level Domain	Network entities (.net)	**DNS Security Extensions**	*unknown*
Hosting country	ID		

Apache : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **1101** Page : 1 (This Page) 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-17197	400			2018-12-24	2019-01-10	4.3	None	Remote	Medium	Not required	None	None	Partial
A carefully crafted or corrupt sqlite file can cause an infinite loop in Apache Tika's SQLite3Parser in versions 1.8-1.19.1 of Apache Tika.														
2	CVE-2018-17195	352		CSRF	2018-12-19	2019-01-11	5.1	None	Remote	High	Not required	Partial	Partial	Partial
The template upload API endpoint accepted requests from different domain when sent in conjunction with ARP spoofing + man in the middle (MiTM) attack, resulting in a CSRF attack. The required attack vector is complex, requiring a scenario with client certificate authentication, same subnet access, and injecting malicious code into an unprotected (plaintext HTTP) website which the targeted user later visits, but the possible damage warranted a Severe severity level. Mitigation: The fix to apply Cross-Origin Resource Sharing (CORS) policy request filtering was applied on the Apache NiFi 1.8.0 release. Users running a prior 1.x release should upgrade to the appropriate release.													
3	CVE-2018-17194	20			2018-12-19	2019-01-11	5.0	None	Remote	Low	Not required	None	None	Partial
When a client request to a cluster node was replicated to other nodes in the cluster for verification, the Content-Length was forwarded. On a DELETE request, the body was ignored, but if the initial request had a Content-Length value other than 0, the receiving nodes would wait for the body and eventually timeout. Mitigation: The fix to check DELETE requests and overwrite non-zero Content-Length header values was applied on the Apache NiFi 1.8.0 release. Users running a prior 1.x release should upgrade to the appropriate release.														
4	CVE-2018-17192	20			2018-12-19	2019-01-11	4.3	None	Remote	Medium	Not required	None	Partial	None
The X-Frame-Options headers were applied inconsistently on some HTTP responses, resulting in duplicate or missing security headers. Some browsers would interpret these results incorrectly, allowing clickjacking attacks. Mitigation: The fix to consistently apply the security headers was applied on the Apache NiFi 1.8.0 release. Users running a prior 1.x release should upgrade to the appropriate release.														
5	CVE-2018-17190	284		Exec Code	2018-11-19	2018-12-17	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
In all versions of Apache Spark, its standalone resource manager accepts code to execute on a 'master' host, that then runs that code on 'worker' hosts. The master itself does not, by design, execute user code. A specially-crafted request to the master can, however, cause the master to execute code too. Note that this does not affect standalone clusters with authentication enabled. While the master host typically has less outbound access to other resources than a worker, the execution of code on the master is nevertheless unexpected.														
6	CVE-2018-14889	20		Exec Code	2018-09-21	2018-11-08	4.6	None	Local	Low	Not required	Partial	Partial	Partial
CouchDB in Vectra Networks Cognito Brain and Sensor before 4.3 contains a local code execution vulnerability.														
7	CVE-2018-11804	20			2018-10-24	2018-12-11	5.0	None	Remote	Low	Not required	Partial	None	None

Citrix » Netscaler : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-6186	918		Exec Code +Priv	2018-02-01	2018-03-02	9.0	None	Remote	Low	Single system	Complete	Complete	Complete
Citrix NetScaler VPX through NS12.0 53.13.nc allows an SSRF attack via the /rapi/read_url URI by an authenticated attacker who has a webapp account. The attacker can gain access to the nsroot account, and execute remote commands with root privileges.														
2	CVE-2016-2072	254			2016-02-17	2016-12-02	4.3	None	Remote	Medium	Not required	None	Partial	None
The Administrative Web Interface in Citrix NetScaler Application Delivery Controller (ADC) and NetScaler Gateway 11.x before 11.0 Build 64.34, 10.5 before 10.5 Build 59.13, 10.5.e before Build 59.1305.e, and 10.1 allows remote attackers to conduct clickjacking attacks via unspecified vectors.														
3	CVE-2016-2071	264		+Priv	2016-02-17	2016-12-02	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Citrix NetScaler Application Delivery Controller (ADC) and NetScaler Gateway 11.x before 11.0 Build 64.34, 10.5 before 10.5 Build 59.13, and 10.5.e before Build 59.1305.e allows remote attackers to gain privileges via unspecified NS Web GUI commands.														
4	CVE-2015-2841	284		Bypass	2015-04-03	2016-12-02	5.0	None	Remote	Low	Not required	None	Partial	None
Citrix NetScaler AppFirewall, as used in NetScaler 10.5, allows remote attackers to bypass intended firewall restrictions via a crafted Content-Type header, as demonstrated by the application/octet-stream and text/xml Content-Types.														
5	CVE-2015-2840	79		XSS	2015-04-03	2018-10-09	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in help/rt/large_search.html in Citrix NetScaler before 10.5 build 52.3nc allows remote attackers to inject arbitrary web script or HTML via the searchQuery parameter.														
6	CVE-2015-2839	79		XSS	2015-04-03	2018-10-09	4.3	None	Remote	Medium	Not required	None	Partial	None
The Nitro API in Citrix NetScaler before 10.5 build 52.3nc uses an incorrect Content-Type when returning an error message, which allows remote attackers to conduct cross-site scripting (XSS) attacks via the file_name JSON member in params/xen_hotfix/0 to nitro/v1/config/xen_hotfix.														
7	CVE-2015-2838	352		Exec Code CSRF	2015-04-03	2018-10-09	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
Cross-site request forgery (CSRF) vulnerability in Nitro API in Citrix NetScaler before 10.5 build 52.3nc allows remote attackers to hijack the authentication of administrators for requests that execute arbitrary commands as nsroot via shell metacharacters in the file_name JSON member in params/xen_hotfix/0 to nitro/v1/config/xen_hotfix.														
8	CVE-2007-6193	200		+Info	2007-11-29	2018-10-15	5.0	None	Remote	Low	Not required	Partial	None	None
The web management interface in Citrix NetScaler 8.0 build 47.8 stores the device's primary IP address in a cookie, which might allow remote attackers to obtain sensitive network configuration														

Igor Sysoev » Nginx : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2013-4547	264		Bypass	2013-11-23	2018-10-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
nginx 0.8.41 through 1.4.3 and 1.5.x before 1.5.7 allows remote attackers to bypass intended restrictions via an unescaped space character in a URI.														
2	CVE-2013-2070	264		DoS +Info	2013-07-19	2018-10-30	5.8	None	Remote	Medium	Not required	Partial	None	Partial
http/modules/ngx_http_proxy_module.c in nginx 1.1.4 through 1.2.8 and 1.3.0 through 1.4.0, when proxy_pass is used with untrusted HTTP servers, allows remote attackers to cause a denial of service (crash) and obtain sensitive information from worker process memory via a crafted proxy response, a similar vulnerability to CVE-2013-2028.														
3	CVE-2013-0337	264		+Info	2013-10-26	2018-10-30	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
The default configuration of nginx, possibly 1.3.13 and earlier, uses world-readable permissions for the (1) access.log and (2) error.log files, which allows local users to obtain sensitive information by reading the files.														
4	CVE-2012-1180	399		+Info	2012-04-17	2018-10-30	5.0	None	Remote	Low	Not required	Partial	None	None
Use-after-free vulnerability in nginx before 1.0.14 and 1.1.x before 1.1.17 allows remote HTTP servers to obtain sensitive information from process memory via a crafted backend response, in conjunction with a client request.														
5	CVE-2009-4487	20		Exec Code	2010-01-13	2018-10-10	5.0	None	Remote	Low	Not required	Partial	None	None
nginx 0.7.64 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.														

Total number of vulnerabilities : 5 Page : 1 (This Page)